UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

CENTER FOR DEMOCRACY & TECHNOLOGY, 1634 I Street, NW, Suite 1100, Washington, DC 20006, on behalf of itself,

AMERICAN CIVIL LIBERTIES UNION OF PENNSYLVANIA, Post Office Box 1161, Philadelphia, PA 19105-161, on behalf of its members, and

PLANTAGENET, INC., 71 North Hamilton Street, Doylestown, PA 18901, on behalf of itself and its customers,

Plaintiffs,

v. No. _____

MICHAEL FISHER, Attorney General of the Commonwealth of Pennsylvania, Strawberry Square Harrisburg, PA 17120,

Defendant.

COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

PRELIMINARY STATEMENT

1. Child pornography is a serious crime, and should have no place in a civilized society. Powerful laws are in place to combat child pornography, and Plaintiffs strongly endorse the full enforcement of such laws. Such enforcement can and should extend to child pornography that may be available over the

Internet – anyone who creates and/or knowingly transmits child pornography over the Internet should be vigorously prosecuted.

2. The Pennsylvania state statute and governmental actions challenged in this Complaint, however, do little or nothing to combat the crime of child pornography or the problem of child pornography on the Internet, notwithstanding the pretense of the statute and actions. Instead, in the name of fighting child pornography, the Defendant Pennsylvania Attorney General has created a completely secret system of prior restraint orders issued to Internet Service Providers with no judicial oversight or review. Moreover, as a result of the technical architecture of the Internet, these prior restraint orders have blocked numerous wholly innocent and fully lawful sites on the Internet's World Wide Web.

3. The actions of the Pennsylvania Attorney General have been taken almost entirely without authorization under Pennsylvania law, completely ignoring the procedures created by the statute he is purporting to enforce. But even the statute itself is constitutionally deficient and would directly lead to the blocking of access to wholly innocent and lawful Internet web sites.

4. The statute and the actions of the Attorney General, separately and taken together, lead to the blocking of access to wholly lawful content not just by Internet users in

Pennsylvania, but also by Internet users elsewhere across the United States.

5. At most, the statute and actions challenged here have only a very small and marginal effect on the problem of child pornography (and in many cases the effect is essentially zero), while at the same time having a much larger negative impact on wholly innocent and lawful speech. In contrast to the statute and actions challenged here, there are a range of possible governmental actions that (a) require the same or significantly less investment of governmental resources, (b) further the governmental interests far more efficiently and effectively than does the statute and actions at issue here, and (c) do so without any adverse affect on wholly innocent and lawful web sites.

JURISDICTION AND VENUE

6. This case arises under the Constitution and laws of the United States and presents a federal question within this Court's jurisdiction under Article III of the Constitution and 28 U.S.C. § 1331.

7. This Court has authority to grant declaratory relief pursuant to the Declaratory Judgment Act, 28 U.S.C. § 2201.

8. Venue is proper in this Court under 28 U.S.C. § 1391(b).

PARTIES

9. Plaintiff CENTER FOR DEMOCRACY & TECHNOLOGY ("CDT") is a non-profit public interest and Internet policy organization, dedicated to promoting an open, decentralized Internet reflecting constitutional and democratic values of free expression, privacy, and individual liberty. CDT is incorporated and has its principle place of business in the District of Columbia. CDT sues on its own behalf.

10. Plaintiff AMERICAN CIVIL LIBERTIES UNION OF PENNSYLVANIA (ACLU-PA) is a nonpartisan organization of more than 13,000 members dedicated to defending the principles of liberty and equality embodied in the Bill of Rights. The ACLU-PA is incorporated in Pennsylvania and has its principal place of business in Philadelphia. The ACLU sues on its own behalf, and on behalf of its members who use online communications.

11. Plaintiff PLANTAGENET, INC., is an Internet Service Provider that provides to its customers access to the Internet through dial-up or dedicated connections, and also offers hosting of web sites on the World Wide Web as well as other Internet services. PLANTAGENET provides local dial-in numbers for most of the greater Philadelphia area, including parts of New Jersey. PLANTAGENET is incorporated in Pennsylvania, and has its principle place of business in Doylestown, Pennsylvania.

PLANTAGENET sues on its own behalf, and on behalf of its customers who obtain access to the Internet through PLANTAGENET.

12. Defendant MICHAEL FISHER is the Attorney General of the Commonwealth of Pennsylvania. Defendant FISHER is directly responsible for the operation of the system of secret prior restraint orders challenged in this Complaint. In addition, Defendant FISHER has statutory responsibility to carry out key elements of the Pennsylvania law also challenged in this Complaint.

FACTS

13. This Complaint challenges two separate governmental actions: (a) a system of secret prior restraint orders undertaken and implemented by Defendant FISHER, and (b) Pennsylvania Statutes, Title 18, §§ 7621-7630, entitled "Internet Child Pornography" (hereafter the "Statute"). The Statute was originally enacted at Pennsylvania Statutes, Title 18, § 7330, but was re-codified in December 2002 at Pennsylvania Statutes, Title 18, §§ 7621-7630.

14. Although Defendant FISHER has asserted that his system of secret prior restraint orders is undertaken pursuant to the Statute, that Statute does not mention or authorize the prior restraint orders that Defendant FISHER issues, and does not

sanction the wholly secret and unreviewable nature of Defendant FISHER's prior restraint system.

15. The Facts in this Complaint are organized into four major sections. First, certain key terms about how one accesses "web sites" on the Internet's World Wide Web are described. Second, Defendant FISHER's system of secret prior restraint orders is described. Third, the provisions of the Statute are described. And fourth, the impact of both (a) the secret prior restraint orders issued by Defendant FISHER, and (b) court orders issued under the Statute, on wholly innocent and lawful speech on the Internet is described.

Critical Terms Concerning the Internet and the World Wide Web

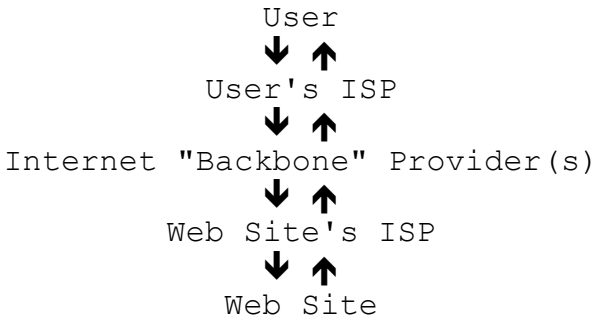
16. The Internet is a global "network of networks" that allows Internet users to send and received a huge diversity of content and communications. The "World Wide Web" is a common method that Internet users can use to make content available to other Internet users. The Internet and the Web have become integral parts of our society.

17. In the United States, most people access the Internet through companies known as Internet Service Providers ("ISPs"). Home Internet users are likely to contract on a monthly or annual basis with an ISP, and will access that ISP's network over a "dial-up" telephone line, or a higher-speed connection

such as a cable or "DSL" circuit. A typical ISP's network is in turn connected, directly or indirectly, to the network of an Internet "backbone" provider, and through the backbone to other ISPs and networks that, collectively, comprise the global Internet.

18. Similarly, businesses in the United States commonly contract with an ISP to provide Internet access to their employees, or to connect their internal computer network to the ISP's network (which is in turn connected to the greater Internet). Many businesses connect to their ISP's networks (and the Internet) over dedicated high-speed connections, while other business access the Internet over dial-up telephone lines.

19. For accessing content on the World Wide Web, the most common sequence is for a user to request content from a "web site," and for the web site to return "web pages" to the user. This sequence is illustrated as follows, with the initial request shown by the arrows on the left, and the response shown by the arrows on the right:



20. In the vast majority of cases, the User's ISP is different from the Web Site's ISP. Thus, the User's ISP does not typically have any knowledge of or relationship with the actual owner of the Web Site.

21. Individuals, businesses, governments, and other institutions (hereafter "Web Publishers") that want to make content broadly available over the Internet can do so by creating a "web site" on the "World Wide Web."

22. To make a web site available on the World Wide Web, a Web Publisher must place the content or "web pages" onto a computer running specialized "web server" software. This computer, known as a "Web Server," transmits the requested web pages in response to requests sent by users on the Internet.

23. Web Publishers have two common options for making a web site available over a Web Server. First, a Web Publisher can own and operate a Web Server on the Web Publisher's premises (including, possibly, the Web Publisher's home). In this case, a Web Publisher would contract with an ISP for Internet access, and would thereby connect the Web Server to the Internet.

24. Second, a Web Publisher may contract with a "Web Host" (or an ISP that also operates as a "Web Host") to own and operate the necessary Web Server on the Web Host's premises (or third party premises arranged by the Web Host). A Web Host will typically operate one or more Web Servers that can store the web

pages for customers and make those web pages generally available to users on the Internet.

25. Typically when creating a Web Site, a Web Publisher obtains a "domain name" that can be used to designate and locate the Web Site. For example, Defendant FISHER obtained the domain name "attorneygeneral.gov" for use with his web site.

26. A domain name can be coupled with additional information to create a "Uniform Resource Locator," or "URL," which represents a more complete way to designate the location of certain content or other resources on the Internet.

27. A URL is the commonly used textual designation of an Internet web site's "address." Thus, for example, the URL of Defendant FISHER's web site is "http://www.attorneygeneral.gov." The "http" indicates that the "Hypertext Transfer Protocol" (which is the main protocol used to transmit World Wide Web pages) is to be used. The "www.attorneygeneral.gov" indicates a name that can be used to locate the specific Web Server(s) that can contain the content for the requested Web Site.

28. A web page accessed by a URL like "http://www.attorneygeneral.gov" is commonly referred to as the "home page" of the web site. A URL could also contain a reference to a specific "sub-page" that is contained in a web site (such as "http://www.attorneygeneral.gov/press/pr.cfm"). A single web site can contain thousands of different web pages.

Although in many cases the same Web Publisher is responsible for all pages and sub-pages on a web site, in other situations (including but not limited to that described in the following paragraph) wholly different and independent Web Publishers are responsible for different sub-pages on a single web site.

29. Beyond the two methods described immediately above, Web Publishers can use a third common method to make web pages available on the World Wide Web. A Web Publisher can place content with a service provider that operates a "community" of users on the Internet and offers to host web pages of the users as part of its service (hereafter "Online Community"). This type of Online Community exists only in "cyberspace," and does not relate to any particular physical community. In the United States, for example, GeoCities is a popular Online Community, and GeoCities hosts web pages of its tens of thousands of users (which commonly are individuals, or very small businesses or organizations). There are also smaller Online Communities that individuals might host out of their homes. A key difference with publishing web content through an Online Community is that Web Publishers' web pages do not typically have their own domain name. For example, the Association of Black Women Lawyers of New Jersey, Inc., is part of the GeoCities Online Community, and its web pages are available at the URL "http://www.geocities.com/abwlnj/homepage.html."

30. Although a URL such as http://www.attorneygeneral.gov or http://www.geocities.com/abwlnj/homepage.html provides enough information for a human user to access the desired Internet web site, the URLs alone are not sufficient for the user's computer to locate the web site. The user's computer must first determine the numeric "Internet Protocol Address" or "IP Address" of the desired web site. When a user seeks to access a particular URL, the user's computer does a "look up" in a series of global databases to determine the IP Address of the computer server that can provide the desired web pages.

31. In the most commonly used method, IP Addresses are expressed as a series of four numbers separated by periods. Thus, for example, the IP Address of the web site designated by http://www.attorneygeneral.gov is 207.102.198.176. This numeric IP Address provides a user's computer with a precise address of the Web Server to which the user's computer must send a request for web pages with the URL http://www.attorneygeneral.gov.

32. For most ISPs, the ISPs receive and forward Internet communications based solely on the IP Address of the destination of the communication, wholly without regard to the specific content of the communication. Thus, a typical ISP would handle an e-mail message addressed to a specific IP Address in exactly the same way that it would handle a web page that is being sent to the same IP Address.

33. Indeed, for most ISPs, the network would not even "read" the content of the communication to be able to determine whether the communication was an e-mail, a web page, or some other type of Internet communication. Moreover, the networks of most ISPs do not even contain the physical equipment that would be necessary to "read" every communication passing through the network and take any action based on the content of the communication.

34. Although a specific URL in general refers only to one specific web site, the same is not true for IP Addresses -- there is not a one-to-one correlation between URLs and IP Addresses. An individual Web Server computer -- with a single IP Address -- can "host" tens, hundreds, or even thousands of different web sites. Thus, many different web sites (each with their own unique URLs) can be hosted on the same physical Web Server, and all can share the same IP Address of that Web Server.

35. For example, 206.112.85.61 is the IP Address of the web site (www.cdt.org) of Plaintiff CDT. But that exact same numeric IP Address is also used by four other web sites (www.ciec.org, www.consumerprivacyguide.org, www.internetpolicy.net, and www.naisproject.org). If a user on the Internet seeks to access CDT's web site, the user's ISP knows only that the user is sending a communication to

206.112.85.61. The user's ISP does not "open" or "read" the communication to determine which specific web site is actually being requested.

36. Although ISPs transport most Internet communications without looking at any information other than the IP Address, a Web Server that supports multiple web sites does "read" the full web request in order to determine which web site is being requested. In the example of www.cdt.org, the web server located at 206.112.85.61 will read any web request it receives to determine which of the five web sites located at that address should be provided.

Defendant FISHER's System of Secret Prior Restraint Orders

37. Following enactment of Pennsylvania Title 18 §§ 7621-7630 (described in the following section), Defendant FISHER decided that he would generally not obtain court orders as permitted by that Statute. Instead, he devised a system of "informal" orders that he issues to Internet Service Providers ("ISPs") without any court or public oversight.

38. In each "informal" order, Defendant FISHER instructs the ISP to block access to one or more specific sites on the Internet's World Wide Web, designated by one or more URLs.

39. For example, on May 20, 2002, Defendant FISHER sent an "informal" order to an ISP located in Virginia. The full text of this "informal" order (with the URL redacted) was:

> This notice is provided to you under the provision of Section 7330 of the Pennsylvania Criminal Code, 18 PACs 7330, and the Internet Child Pornography [sic].
>
> This notice is further provided to you to advise you that child pornography, as defined at Section 6312 of the Pennsylvania Crime Code, 18 PACs 6312, has been [accessed] through your service at uniform resource locator [redacted].
>
> You must remove or disable access to those items identified as child pornography to your subscribers who subscribe to your service from an address located within the Commonwealth of Pennsylvania within five business days of receipt of this notice.
>
> You must ensure that: 1. Access to uniform resources locator [redacted] be denied to your subscribers to your services from an address located within the Commonwealth of Pennsylvania using Internet services provided by [sic] and that the Attorney General or his designated agent is notified in writing (e-mail, fax) that you have complied with this Informal Notice within five business days of said compliance. 2. Accompanying this compliance notification should be a screen shot of the resource locator demonstrating that access have [sic] been disabled.

40. Since April 2002, Defendant FISHER has sent more than 300 prior restraint orders similar to the one quoted above, and has through those orders targeted more than 400 different Internet URLs.

41. The vast majority of the 300+ prior restraint orders instructed ISPs to block Internet content that was hosted and physically located elsewhere on the Internet.

42. Fewer than ten of the 300+ prior restraint orders have been directed to Web Publishers that do not appear themselves to operate as ISPs as that term is commonly understood.

43. Defendant FISHER issues these prior restraint orders without any judicial review of his assertion that the web sites targeted in the orders are unlawful. No court reviews the orders either before or after they are issued.

44. Although some of the 300+ "informal" prior restraint orders reference Section 7330 of the Pennsylvania Criminal Code (the original citation for the Statute, which is now found at Title 18, Sections 7621-7630), none of the orders were, at the time they were issued, issued in connection with a court order under that Statute or as a result of any other judicial proceeding. As described more fully in Paragraphs 57-62 below, in only one instance relating to approximately five of the 300+ "informal orders," did Defendant FISHER subsequently seek a court order under the Statute addressing the same URLs as were referenced in the "informal orders."

45. No ISP or web site receives any prior notice before Defendant FISHER issues a prior restraint order, and no ISP or

web site is afforded an opportunity to participate in any adversarial proceeding prior to the issuance of an order.

46. Defendant FISHER provides no notice to the affected web sites even after the issuance of a prior restraint order.

47. Defendant FISHER operates his system of prior restraints in a secret manner. At no time does FISHER inform the public of what Internet content he has blocked.

48. In February 2003, Plaintiff CDT assisted in the submission of a Pennsylvania Right to Know Law request to Defendant FISHER, seeking the identity of the URLs that FISHER had blocked using the secret prior restraint orders. Defendant FISHER partially denied the Right to Know Law request, producing copies of the prior restraint orders but redacting the URLs from those orders. As justification for the partial denial, Defendant FISHER asserted that the mere act of disclosing the URLs would constitution the distribution of child pornography under Pennsylvania law. Although Plaintiff CDT believes that Defendant FISHER's partial denial of the Right to Know Law request violates Pennsylvania law, that state law issue is not raised in this action.

49. Defendant FISHER has maintained his system of secret prior restraint orders through intimidation of ISPs. After one ISP, WorldCom, wrote to Defendant FISHER to suggest that FISHER should use the statutory procedures instead of the secret prior

restraint orders, Defendant FISHER issued a press release accusing the ISP of refusing to block child pornography.

50. Since the issuance of the press release attacking WorldCom, no ISP has refused to follow any of the secret prior restraint orders. ISPs understand that if they do not comply with Defendant FISHER's "informal" orders, FISHER will publicly describe the ISPs as supporting child pornography, even though the ISPs have no responsibility for or involvement with the alleged child pornography. Defendant FISHER has maintained his system of secret censorship through intimidation and coercion of the ISPs.

51. The facts surrounding Defendant FISHER's system of "informal" prior restraint orders are remarkably similar to the facts held by the United States Supreme Court to be unconstitutional in *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58 (1963), except that the prior restraint orders held to be unconstitutional in *Bantam Books* were not issued in secret, as they are here.

Pennsylvania Statutes, Title 18, Section 7621-7630

52. The secret prior restraint orders are not mentioned in or sanctioned by the statute that Defendant FISHER is claiming to enforce through his secret orders. Pennsylvania Statutes, Title 18, Sections 7621-7630 (the "Statute") does not support

the Defendant's actions. The provisions established in the Statute, however, are also constitutionally inadequate.

53. The Statute is reproduced in its entirety in the Statutory Appendix to this Complaint. The most relevant provisions of the Statute are:

> **§ 7622. DUTY OF INTERNET SERVICE PROVIDER**
> AN INTERNET SERVICE PROVIDER SHALL REMOVE OR DISABLE ACCESS TO CHILD PORNOGRAPHY ITEMS RESIDING ON OR ACCESSIBLE THROUGH ITS SERVICE IN A MANNER ACCESSIBLE TO PERSONS LOCATED WITHIN THIS COMMONWEALTH WITHIN FIVE BUSINESS DAYS OF WHEN THE INTERNET SERVICE PROVIDER IS NOTIFIED BY THE ATTORNEY GENERAL PURSUANT TO SECTION 7628 (RELATING TO NOTIFICATION PROCEDURE) THAT CHILD PORNOGRAPHY ITEMS RESIDE ON OR ARE ACCESSIBLE THROUGH ITS SERVICE.
>
> **§ 7624. PENALTY**
> NOTWITHSTANDING ANY OTHER PROVISION OF LAW TO THE CONTRARY, ANY INTERNET SERVICE PROVIDER WHO VIOLATES SECTION 7622 (RELATING TO DUTY OF INTERNET SERVICE PROVIDER) COMMITS [a misdemeanor for a first and second offense, and for a third offense a felony punishable by a fine of $30,000 and seven years in prison].
>
> **§ 7625. JURISDICTION FOR PROSECUTION**
> THE ATTORNEY GENERAL SHALL HAVE CONCURRENT PROSECUTORIAL JURISDICTION WITH THE COUNTY DISTRICT ATTORNEY FOR VIOLATIONS OF THIS SUBCHAPTER. . . .
>
> **§ 7626. APPLICATION FOR ORDER TO REMOVE OR DISABLE ITEMS**
> AN APPLICATION FOR AN ORDER OF AUTHORIZATION TO REMOVE OR DISABLE ITEMS RESIDING ON OR ACCESSIBLE THROUGH AN INTERNET SERVICE PROVIDER'S SERVICE SHALL BE MADE TO THE COURT OF COMMON PLEAS HAVING JURISDICTION IN WRITING UPON THE PERSONAL OATH OR AFFIRMATION OF THE ATTORNEY GENERAL OR A DISTRICT ATTORNEY OF THE COUNTY WHEREIN THE ITEMS HAVE BEEN DISCOVERED AND, IF

AVAILABLE, SHALL CONTAIN ALL OF THE FOLLOWING INFORMATION:

(1) A statement of the authority of the applicant to make such an application.

(2) A statement of the identity of the investigative or law enforcement officer that has, in the official scope of that officer's duties, discovered the child pornography items.

(3) A statement by the investigative or law enforcement officer who has knowledge of relevant information justifying the application.

(4) The Uniform Resource Locator providing access to such items.

(5) The identity of the Internet Service Provider used by the law enforcement officer.

(6) A showing that there is probable cause to believe that such items constitute a violation of section 6312 (relating to sexual abuse of children).

(7) A proposed order of authorization for consideration by the judge.

(8) Contact information for the Office of Attorney General, including the name, address and telephone number of any deputy or agent authorized by the Attorney General to submit notification.

(9) Additional testimony or documentary evidence in support of the application as the judge may require.

§ 7627. ORDER TO REMOVE OR DISABLE CERTAIN ITEMS FROM INTERNET SERVICE PROVIDER'S SERVICE

UPON CONSIDERATION OF AN APPLICATION, THE COURT MAY ENTER AN ORDER, INCLUDING AN EX PARTE ORDER AS REQUESTED, ADVISING THE ATTORNEY GENERAL OR A DISTRICT ATTORNEY THAT THE ITEMS CONSTITUTE

> PROBABLE CAUSE EVIDENCE OF A VIOLATION OF SECTION 6312 (RELATING TO SEXUAL ABUSE OF CHILDREN) AND THAT SUCH ITEMS SHALL BE REMOVED OR DISABLED FROM THE INTERNET SERVICE PROVIDER'S SERVICE. THE COURT MAY INCLUDE SUCH OTHER INFORMATION IN THE ORDER AS THE COURT DEEMS RELEVANT AND NECESSARY.
>
> **§ 7628. NOTIFICATION PROCEDURE**
> (a) DUTY OF ATTORNEY GENERAL.--THE ATTORNEY GENERAL SHALL HAVE EXCLUSIVE JURISDICTION TO NOTIFY INTERNET SERVICE PROVIDERS UNDER THIS SUBCHAPTER. . . .

54. Section 7627 of the Statute permits the entry of an ex parte court order requiring that an ISP block access to certain Internet content. Under the statute, no notice is required to any ISP or web site affected by an order (and no notice is provided to any affected web sites following the entry of an order).

55. Section 7627 of the Statute requires only that the court find that there exists "probable cause evidence" that certain Internet content violates the Pennsylvania child pornography statute. The Statute does not provide for any further proceedings after a probable cause order is entered. At no point is there any definitive judicial determination that any particular content is in fact unlawful.

56. Section 7621 of the Statute defines "Internet Service Provider" to be any "person who provides a service that enables users to access content, information, electronic mail or other services offered over the Internet." This definition is broad

enough to include any company or organization that provides Internet access to its employees.

57. The Statute has to date only been used one time. In September 2002, Defendant FISHER obtained an ex parte probable cause order against the ISP WorldCom, after WorldCom indicated in July 2002 that it would not comply with the statutorily-unauthorized secret prior restraint orders described above.

58. Appended to this ex parte probable cause court order was the July 2002 letter sent by WorldCom to the staff of Defendant FISHER. In that letter, WorldCom states:

> As we also have discussed with your colleagues at various times, please note that due to WorldCom's network architecture, it is not technically-feasible for us to block access to a site on the Internet based on the URL of that site; rather, the only technically-feasible solution for WorldCom to block access to a site not on our network is by means of null routing the Internet Protocol number of the site in question.

59. The network architecture of the WorldCom Internet network is similar to and consistent with the architecture of most ISPs that provide Internet access. Because (as described a above at paragraphs 32-36) common ISPs receive and forward Internet communications based solely on the IP Address (and wholly without regard to content such as the URL of the specific web site being transmitted), WorldCom is unable to block Internet communications based on the specific URL of the a page

in the communication. Thus, WorldCom, like most ISPs, can only comply with a content blocking order by blocking access to the entire IP Address used by the specific URL targeted in the order.

60. The ex parte probable cause court order was titled "Order Requiring an Internet Service Provider to Remove or Disable Access to Child Pornography," and was entered on September 17, 2002, by the Court of Common Pleas of Montgomery County, Pennsylvania, in In the Matter of the Application of D. Michael Fisher, Attorney General of the Commonwealth of Pennsylvania for an Order Requiring an Internet Service Provider to Remove or Disable Access to Child Pornography, No. Misc 689 Jul 02, Ct. Cm. Pleas, Montgomery County, Pa.

61. The ex parte probable cause court order required that WorldCom block access to five web pages designated by URLs. Of the five URLs provide, two targeted what appears to be the top "page" of a web site (often termed the "homepage"), while three targeted what appears to be individual "sub-pages" under the home page. For the three URLs for which only sub-pages were targeted, neither the application nor the court's order made any assertion or determination as to the lawfulness of the content located on other pages of the targeted web sites.

62. As an example, the ex parte probable cause court order requires WorldCom to block the following URL:

http://www.terra.es/personal8/jenout/

The "terra.es" web site operates one of the largest Spanish language "Online Communities" in the world. As such, terra.es provides to tens of thousands of users the opportunity to create a "personal web page." The page targeted by the ex parte probable cause court order was one of thousands of personal web pages hosted by terra.es. The court order did not make any determination as to the lawfulness of the thousands of other web pages that are located at URL "http://www.terra.es."

The Impact on Wholly Innocent and Lawful Web Sites

63. Both the secret prior restraint orders issued by Defendant FISHER, and court orders entered under the Statute, have the same basic impact on the Internet in general, and on lawful web sites in particular. Both types of orders require an ISP to block access to specified URLs on the Internet. For purposes of this section of the Complaint, both types of order shall be referred to collectively as "Orders" or an "Order."

64. Most ISPs cannot as a technical matter effectively comply with an Order by blocking content based on the specific URL of a web site or a web page. To effectively comply with an Order, most ISPs can only block access to a web site by blocking access to the numeric "IP Address" of the web site.

65. To effectively comply with an Order, most ISPs would be forced to create an "exception" in a "routing table" in order to "null route" or "mis-route" Internet traffic associated with the IP Address.

66. Blocking access to an IP Address will block access to all web sites that use that IP Address, including web sites that are wholly unrelated to any URLs listed in any Order.

67. The sharing of IP Addresses among wholly unrelated web sites is a very common practice on the Internet today.

68. According to recent research, over 85% of all Internet web sites that have domain names ending in ".com," ".net," or ".org" share their IP Addresses with at least one other Internet web site.

69. According to recent research, over 66% of all Internet web sites that have domain names ending in ".com," ".net," or ".org" share their IP Addresses with at least fifty other Internet web sites.

70. In some cases, hundreds and even thousands of web sites share a single IP Address.

71. In most cases, the web sites that share their IP Address with dozens or hundreds of other web sites have no affiliation or relationship with the other web sites that share their IP Address.

72. Internet web sites that carry hard core pornographic sexual content can share their IP Address with unrelated non-sexual web sites.

73. IP Address 206.168.98.228 provides a good illustration of IP Address sharing. That IP Address is used by over 400 unrelated web sites including a variety of hard core sexually oriented web sites, such as

www.1-800-phone-sex.com
www.all-fetishes-phone-sex.com
www.mommy-phone-sex.com
www.nof~~~ingaround.com (sexual site name redacted)
www.phone-sex-kittens.com
www.spermbreath.com
www.suddentemptation.com

as well as a diversity of web sites that are wholly non-sexual, including

www.atonementgreenbay.org (church, WI)
www.candymountaindaycamp.com (day camp, NY)
www.christiannewswatch.com (news service, Mumbai, India)
www.doubledutchconstruction.com (construction co., MN)
www.funeralconsumersphila.org (consumers org., PA)
www.huckfinncharters.com (boat charters, NC)
www.mozartforchildren.com (music school, NY)
www.northshorerotary.net (civic club, NJ)
www.prayer-sisters.com (online prayer site)
www.vfw4250.org (veterans org., FL)
www.virginiafamilyrealtors.com (realtor, VA).

74. Any Order targeted at any one of the 400+ sites that use IP Address 206.168.98.228 would have the effect of blocking access to all 400+ sites. Thus, an Order to block access to, for example, "www.mommy-phone-sex.com," would result in the

blocking of "www.northshorerotary.net," "www.prayer-sisters.com," and hundreds of other unrelated web sites.

75. Orders sent to most ISPs targeting a particular URL are very likely to lead to the blocking of access to wholly unrelated web sites that share the IP Address of the targeted URL.

76. In some cases an ISP might be wholly unable to control access based on IP Address, and thus would be unable to comply fully and reliably with Orders at issue in the Complaint. In some of these cases, the ISP may be able to attempt partial compliance with such Orders by "spoiling" or manipulating a table used in the "domain name lookup" process.

77. Such an approach would still result in the blocking of access to lawful Internet content, because under such an approach the ISP would have to block access to all portions of a web site, even if a blocking Order only required blocking of a specific subpage of the web site.

78. For regional or national ISPs, any action taken to comply with an Order will affect the Internet access of customers both in Pennsylvania and in other states around the country (and in some cases in other countries). In other words, content blocked as a result of a Pennsylvania Order will be blocked far outside of Pennsylvania's borders.

79. Specifically, the Orders challenged in this Complaint have a direct and significant harmful affect on interstate and foreign commerce and communications. In almost all (if not all) cases, the Orders challenged in this Complaint interfere with the ability of Internet users located outside of Pennsylvania to access content also located outside of Pennsylvania. In most cases the communications obstructed by the Orders would have taken place (but for the Orders) entirely outside of the borders of Pennsylvania.

80. The Orders at issue in this Complaint have directly led to the blocking of wholly innocent and lawful web sites on the Internet.

81. On information and belief, wholly innocent and lawful web sites on the Internet are currently being blocked today as a result of the Orders at issue in this Complaint.

82. Because of the secret nature of Defendant Fisher's system of prior restraint orders, most of the innocent web sites that have been or are being blocked as a result of the Orders at issue in this Complaint are not publicly known. The following web sites are examples of the innocent and wholly lawful sites known to have been blocked as a result of the Orders:

* Web site of the Bioterrorism Safety Council, at http://www.terra.es/personal5/safetycouncil/

* Web site of the ITGE Geological Survey of Spain, at http://www.terra.es/personal/lsomoza/marina/proyectos.html

* Web site of Our Lady of Mercy, an English speaking Roman Catholic Church in Madrid, Spain, at http://www.terra.es/personal/ourladyofmercy/

* Web site of the International Philatelic Club, at http://www.terra.es/personal/jla31291/home.htm

* Web sites of numerous hotels and tourist locations targeting English speaking travelers, including for example the Hotel Rural Era de La Corte, at http://www.terra.es/personal/eradelacorte/ingles.htm

83. Various citizens of and organizations located in Pennsylvania operate web sites that themselves link to wholly innocent and lawful web sites that have been blocked by the Orders at issue in this Complaint. For example, the following are examples of web sites operated by or affiliated with leading colleges and universities in Pennsylvania that contain links to lawful web sites that have been blocked by the Orders:

* Bryn Mawr College Spanish Department, at http://www.brynmawr.edu/spanish/dbrena/modism%20links.htm

* The Reginald H. Jones Center for Management Policy, Strategy, and Organization of the Wharton School of the University of Pennsylvania, at http://jonescenter.wharton.upenn.edu/VirtualCommunities/amit.pdf

* Doctoral candidate at Penn State University, at http://www.personal.psu.edu/users/j/s/jsr199/publications/iallj_33_2.pdf

Similarly, wholly innocent web sites that have been blocked by Orders are also linked to by lower level educational

institutions in Pennsylvania, including for example, http://sasd.k12.pa.us/Academics/SpecialEducation/gatehunt/wondersealstrikeswithalargeplateofcheese.html.

84. In contrast to the harm caused by the Orders to lawful speech on the Internet, the Orders do very little to harm the creators and knowing distributors of the child pornography that is alleged to exist at the URLs targeted in the Orders.

85. No investigation or prosecution of the creators and knowing distributors results from the Orders.

86. Child pornography is illegal in all or almost all countries of the world.

87. The vast majority of ISPs in the world do not permit the use of their services to host or deliver child pornography.

88. The vast majority of ISPs in the world will take action to remove alleged child pornography if they are contacted by a law enforcement official.

89. There exists a range of possible governmental actions that (a) require the same or significantly less investment of governmental resources than required to obtain an order under the Statute, (b) further the governmental interests far more efficiently and effectively than does the Orders at issue here, and (c) do so without any adverse affect on wholly innocent and lawful web sites.

90. Among the less restrictive alternative government actions are (a) directly contacting the Web Host (or hosting ISP) about the alleged child pornography, to seek to have the content removed at the source, and (b) working with national and international investigators, including the Federal Bureau of Investigation and the U.S. Customs Service, to investigate and prosecute the creators and knowing distributors of child pornography.

91. Plaintiff CENTER FOR DEMOCRACY & TECHNOLOGY ("CDT") obtains its Internet access from WorldCom, an ISP that has received both secret prior restraint orders issued by Defendant FISHER and an order issued under the Statute. Thus, even though the operations of CDT are almost entirely outside of the state of Pennsylvania, the ability of CDT and its employees to access lawful content over the Internet is directly harmed by the blocking of lawful content that has resulted from or may in the future result from the orders challenged in this Complaint.

92. Plaintiff AMERICAN CIVIL LIBERTIES UNION OF PENNSYLVANIA (ACLU-PA), and its Pennsylvania members who use online communications, all obtain their Internet access from ISPs that have received or may receive either secret prior restraint orders issued by Defendant FISHER or orders issued under the Statute. Thus, the ability of ACLU-PA and its Pennsylvania members to access lawful content over the Internet

is directly harmed by the blocking of lawful content that has resulted from and may in the future result from the orders challenged in this Complaint.

93. In addition, in light of the breadth of the definition of "Internet Service Provider" in Section 7621 and the diversity of the entities that have received secret prior restraint orders from Defendant FISHER, Plaintiff AMERICAN CIVIL LIBERTIES UNION OF PENNSYLVANIA (ACLU-PA) also has a reasonable fear that it could receive and be directly subject to either a prior restraint order issued by Defendant FISHER or a court order issued pursuant to the Statute.

94. Plaintiff PLANTAGENET, INC., provides Internet access to customers in Pennsylvania, and is an "Internet Service Provider" under the definition in Section 7621 of the Statute. As such, Plaintiff PLANTAGENET has a reasonable fear that it will receive one or both of the two types of Orders challenged in this Complaint. Because of the structure of its operations, PLANTAGENET has no direct ability to comply with any such Order, and would thus be at risk of criminal liability if it becomes subject to an Order.

CAUSES OF ACTION

COUNT 1

95. Plaintiffs repeat and reallege paragraphs 1-94.

96. Both the secret blocking orders created and used by Defendant FISHER, and orders issued pursuant to the Statute, operate as an unconstitutional prior restraint, and thereby deprive Plaintiffs and their members and customers of access to constitutionally protected content, in violation of the First Amendment of the United States Constitution.

COUNT 2

97. Plaintiffs repeat and reallege paragraphs 1-94.

98. Both the secret blocking orders created and used by Defendant FISHER, and orders issued pursuant to the Statute, unduly burden a substantial amount of lawful speech by and to Internet users, including Plaintiffs and their members and customers, in violation of the First Amendment of the United States Constitution.

COUNT 3

99. Plaintiffs repeat and reallege paragraphs 1-94.

100. The secret blocking orders created and used by Defendant FISHER establish a system of secret censorship, and the secrecy alone violates the constitutional right of Internet users, including Plaintiffs and their members and customers, to know what is being censored by the government.

COUNT 4

101. Plaintiffs repeat and reallege paragraphs 1-94.

102. Both the secret blocking orders created and used by Defendant FISHER, and orders issued pursuant to the Statute, afford ISPs, Internet content publishers, and Internet users, including Plaintiffs and their members and customers, inadequate procedural protection of their rights, in violation of the First and Fourteenth Amendments of the United States Constitution.

COUNT 5

103. Plaintiffs repeat and reallege paragraphs 1-94.

104. Both the secret blocking orders created and used by Defendant FISHER, and orders issued pursuant to the Statute, have a significant harmful effect on interstate commerce because they interfere with commercial and other speech of both Internet speakers and listeners, including Plaintiffs and their members and customers, beyond the borders of Pennsylvania, in violation of the Commerce Clause of the of the United States Constitution.

WHEREFORE, Plaintiffs respectfully pray that this Court:

A. Declare that (a) the secret prior restraint orders issued by Defendant FISHER, and (b) Sections 7621-7630 of Pennsylvania Statutes, Title 18, are unconstitutional;

B. Preliminarily and permanently enjoin Defendant FISHER from issuing any secret prior restraint orders or enforcing Sections 7621-7630 of Pennsylvania Statutes, Title 18;

C. Declare that all prior secret prior restraint orders or orders under Sections 7621-7630 of Pennsylvania Statutes, Title 18, are unconstitutional, void, and unenforceable;

D. Award Plaintiffs such costs and fees pursuant to 42 U.S.C. § 1988 and other applicable by law; and

E. Grant plaintiffs such other and further relief as the Court deems just and proper.

Respectfully Submitted,

_____
John B. Morris, Jr., Esq.
Lara M. Flint, Esq.
Center for Democracy & Technology
1634 I Street, NW, Suite 1100
Washington, D.C. 20006
(202) 637-9800

_____
Stefan Presser, Esq.
Bar No. 43067
Legal Director
American Civil Liberties Union
of Pennsylvania
125 South Ninth Street
Suite 701
Philadelphia, PA 19107
(215) 592-1513 ext. 116

Seth Kreimer, Esq.
Bar No. 26102
3400 Chestnut Street
Philadelphia, PA 19104
(215) 898-7447

Dated: September 9, 2003

STATUTORY APPENDIX

18 Pennsylvania Statutes §§ 7621-7630

TITLE 18. CRIMES AND OFFENSES
PART II. DEFINITION OF SPECIFIC OFFENSES
ARTICLE G. MISCELLANEOUS OFFENSES
CHAPTER 76. COMPUTER OFFENSES
SUBCHAPTER C. INTERNET CHILD PORNOGRAPHY

§ 7621. Definitions

The following words and phrases when used in this subchapter shall have the meanings given to them in this section unless the context clearly indicates otherwise:

"Child pornography." As described in section 6312 (relating to sexual abuse of children).

"Internet." The myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected worldwide network of networks that employ the transmission control protocol/Internet protocol or any predecessor or successor protocols to such protocol to communicate information of all kinds by wire or radio.

"Internet service provider." A person who provides a service that enables users to access content, information, electronic mail or other services offered over the Internet.

§ 7622. Duty of Internet service provider

An Internet service provider shall remove or disable access to child pornography items residing on or accessible through its service in a manner accessible to persons located within this Commonwealth within five business days of when the Internet service provider is notified by the Attorney General pursuant to section 7628 (relating to notification procedure) that child pornography items reside on or are accessible through its service.

§ 7623. Protection of privacy

Nothing in this subchapter may be construed as imposing a duty on an Internet service provider to actively monitor its service or affirmatively seek evidence of illegal activity on its service.

§ 7624. Penalty

Notwithstanding any other provision of law to the contrary, any Internet service provider who violates section 7622 (relating to duty of Internet service provider) commits:

(1) A misdemeanor of the third degree for a first offense punishable by a fine of $ 5,000.

(2) A misdemeanor of the second degree for a second offense punishable by a fine of $ 20,000.

(3) A felony of the third degree for a third or subsequent offense punishable by a fine of $ 30,000 and imprisonment for a maximum of seven years.

§ 7625. Jurisdiction for prosecution

The Attorney General shall have concurrent prosecutorial jurisdiction with the county district attorney for violations of this subchapter. No person charged with a violation of this subchapter by the Attorney General shall have standing to challenge the authority of the Attorney General to prosecute the case. If a challenge is made, the challenge shall be dismissed and no relief shall be available in the courts of this Commonwealth to the person making the challenge.

§ 7626. Application for order to remove or disable items

An application for an order of authorization to remove or disable items residing on or accessible through an Internet service provider's service shall be made to the court of common pleas having jurisdiction in writing upon the personal oath or affirmation of the Attorney General or a district attorney of the county wherein the items have been discovered and, if available, shall contain all of the following information:

(1) A statement of the authority of the applicant to make the application.

(2) A statement of the identity of the investigative or law enforcement officer that has, in the official scope of that officer's duties, discovered the child pornography items.

(3) A statement by the investigative or law enforcement officer who has knowledge of relevant information justifying the application.

(4) The Uniform Resource Locator providing access to the items.

(5) The identity of the Internet service provider used by the law enforcement officer.

(6) A showing that there is probable cause to believe that the items constitute a violation of section 6312 (relating to sexual abuse of children).

(7) A proposed order of authorization for consideration by the judge.

(8) Contact information for the Office of Attorney General, including the name, address and telephone number of any deputy or agent authorized by the Attorney General to submit notification.

(9) Additional testimony or documentary evidence in support of the application as the judge may require.

§ 7627. Order to remove or disable certain items from Internet service provider's service

Upon consideration of an application, the court may enter an order, including an ex parte order as requested, advising the Attorney General or a district attorney that the items constitute probable cause evidence of a violation of section 6312 (relating to sexual abuse of children) and that such items shall be removed or disabled from the Internet service provider's service. The court may include such other information in the order as the court deems relevant and necessary.

§ 7628. Notification procedure

(a) DUTY OF ATTORNEY GENERAL.--THE ATTORNEY GENERAL SHALL HAVE EXCLUSIVE JURISDICTION TO NOTIFY INTERNET SERVICE PROVIDERS UNDER THIS SUBCHAPTER. THE ATTORNEY GENERAL SHALL INITIATE NOTIFICATION UNDER THIS SUBCHAPTER IF REQUESTED IN WRITING BY A DISTRICT ATTORNEY WHO HAS PROVIDED THE ATTORNEY GENERAL WITH A COPY OF AN APPLICATION MADE UNDER SECTION 7626 (RELATING TO APPLICATION TO REMOVE OR DISABLE ITEMS) AND A COPY OF THE ORDER ISSUED UNDER SECTION 7627 (RELATING TO ORDER TO REMOVE OR DISABLE CERTAIN ITEMS FROM INTERNET SERVICE PROVIDER'S SERVICE) OR UPON THE ISSUANCE OF AN ORDER BASED UPON AN APPLICATION FILED BY THE ATTORNEY GENERAL.

(b) TIMELY NOTIFICATION.--FOR PURPOSES OF THIS SECTION, AN INTERNET SERVICE PROVIDER OR THE PERSON DESIGNATED BY THE INTERNET SERVICE PROVIDER AS PROVIDED FOR IN SECTION 7629 (RELATING TO DESIGNATED AGENT) SHALL BE NOTIFIED IN WRITING BY THE ATTORNEY GENERAL WITHIN THREE BUSINESS DAYS OF THE ATTORNEY GENERAL'S RECEIPT OF AN ORDER.

(c) CONTENTS.--THE NOTICE SHALL INCLUDE THE FOLLOWING INFORMATION:

(1) A copy of the application made under section 7626.

(2) A copy of the court order issued under section 7627.

(3) Notification that the Internet service provider must remove or disable the items residing on or accessible through its service within five business days of the date of receipt of the notification.

(4) Contact information for the Office of Attorney General, including the name, address and telephone number of any deputy or agent authorized by the Attorney General to submit notification pursuant to this subsection.

§ 7629. Designated agent

An Internet service provider may designate an agent to receive notification provided under section 7628 (relating to notification procedure).

§ 7630. Report to General Assembly

The Attorney General shall make an annual report to the chairman and minority chairman of the Judiciary Committee of the Senate and to the chairman and minority chairman of the Judiciary Committee of the House of Representatives providing information on the number of notifications issued and the prosecutions made under this subchapter and making any recommendations for amendatory language.